IN THE CLAIMS

1. (currently amended) A digital signature method for a network infrastructure copy protection system, comprising ~~the steps of~~:

~~a)~~ applying a digital signature to a digital content file;

~~b)~~ transmitting the content file across a distributed computer network;

~~c)~~ examining the content file to determine whether the content file includes the digital signature, the examining performed within the distributed computer network;

~~d)~~ transmitting the content file when the content file includes the digital signature; ~~and~~

~~e)~~ blocking transmission of the content file when the content file does not include the digital signature; and

blocking transmission of the content file when the content file comprises a restricted data format.

2. (original) The method of Claim 1 wherein the digital signature is configured to identify the sender of the digital content file.

3. (original) The method of Claim 1 further including the step of logging the digital signature applied to the content file within the distributed computer network when the content file is transmitted across the distributed computer network.

4. (original) The method of Claim 1 wherein the distributed computer network is the Internet.

5. (original) The method of Claim 1 wherein the examining is performed by a plurality of routers within the distributed computer network.

6. (original) The method of Claim 1 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

7. (currently amended) A restricted data format method for a network infrastructure copy protection system, comprising ~~the steps of~~:

~~a)~~ receiving a digital content file for transmission across a distributed computer network;

~~b)~~ examining the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network;

~~c)~~ transmitting the content file when the content file does not include the restricted data format; and

~~d)~~ blocking transmission of the content file when the content file does include the restricted data format.

8. (original) The method of Claim 7 wherein the restricted data format includes MP3 data formats.

9. (original) The method of Claim 7 wherein the restricted data format includes MPEG video data formats.

10. (original) The method of Claim 7 wherein the restricted data format includes Word Document formats.

11. (original) The method of Claim 7 wherein the distributed computer network is the Internet.

12. (original) The method of Claim 7 wherein the examining is performed by a plurality of routers within the distributed computer network.

13. (original) The method of Claim 7 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

---

14. (new) The method of Claim 1 wherein the restricted data format is an MP3 data format.

15. (new) The method of Claim 1 wherein the restricted data format is an MPEG video data format.

16. (new) The method of Claim 1 wherein the restricted data format is a Word document format.

17. (new) A network infrastructure protection method for detecting and denying transmission of restricted data formats, comprising:

receiving a content file for transmission across a distributed computer network;

examining the content file to determine whether the content file comprises a restricted data format, the examining performed within the distributed computer network;

A1

transmitting the content file when the content file does not include the restricted data format; and

blocking transmission of the content file when the content file does include the restricted data format.

A3

18. (new) The method of Claim 17 wherein the restricted data format is an MP3 data format.

19. (new) The method of Claim 17 wherein the restricted data format is an MPEG video data format.

20. (new) The method of Claim 17 further comprising:

examining the file to determine whether the file includes a valid digital signature.